

CLAIMS

What is claimed is:

- sub 1
C1
- 1 1. An ephemeral-output-only browser. Netscape
- 1 2. A system for protecting content distributed through a network comprising:
2 a client computer operable for connecting to the network and for executing a
3 client program that limits user control over the content distributed through the network;
4 and
5 a server computer operable for connecting to the network and for executing a
6 security program for securing the content distributed through the network.
- 1 3. The system of claim 2, wherein the client program is an ephemeral-output-only
2 web browser.
- 1 4. The system of claim 2, wherein the client program is an add-in security module
2 for executing as part of a standard web browser and wherein user control over
3 reproduction of the content, in at least one form, is limited.
- 1 5. The system of claim 2, wherein the client program executes as a separate window
2 in a standard web browser and wherein user control over reproduction of the content, in at
3 least one form, is limited.
- sub 1
C2
- 1 6. The system of claim 2, wherein the security program distributes the content to the
2 client computer only when the client computer is executing the client program, in at least
3 one form, is limited.

1 7. The system of claim 2, wherein the security program secures the content using a
2 common security model.

1 8. The system of claim 2, wherein the security program secures a portion of the
2 content using an individual security model.

1 9. The system of claim 2, wherein the client program limits user control over the
2 content through a technique chosen from the group consisting of:

3 message monitoring, clipboard flushing, function disabling, source code
4 encryption, content localization, secure document packaging, cache encryption, and
5 device content monitoring,

6 and wherein user control over reproduction of the content in any non-ephemeral
7 output manner is prevented.

1 10. A method of enabling a provider to protect content distributed on a network
2 comprising:

3 acquiring a server security program;

4 executing the server security program on a server computer connected to the
5 network; and

6 distributing the content only to a client computer executing a limited-user client
7 program which limits reproduction of the content in at least one form.

1 11. The method of claim 10, further comprising:

2 acquiring a plurality of copies of the limited-user client program; and

3 downloading one of the plurality of copies to the client computer.

1 12. The method of claim 10, wherein distributing the content comprises:

2 obtaining a promise of compensation from a user of the client computer.

1 13. The method of claim 12, wherein the compensation is a one-time fee.

1 14. The method of claim 12, wherein the compensation is a subscription fee.

1 15. The method of claim 12, wherein the compensation is a per-session fee.

1 16. The method of claim 12, wherein the compensation is a per-access fee.

1 17. The method of claim 12, wherein the limited-use client program disables a certain
2 user function and the compensation comprises a fee for re-enabling the certain user
3 function.

1 18. The method of claim 17, wherein the certain user function modifies the content.

1 19. The method of claim 17, wherein the certain user function copies the content to a
2 different medium.

1 20. *It should be restriction* A method of receiving compensation for a security system for protecting content
2 distributed on a network comprising:
3 selling a server security program to a content provider; and
4 selling a plurality of copies for a limited-use client program to the content
5 provider for licensing to users wishing to access the content.

1 21. The method of claim 20, wherein the compensation is received at least from one
2 of (a) when the server security program is executed by the content provider and (b) when
3 the content provider licenses one of the plurality of copies.

1 22. The method of claim 20, wherein the server security program distributes the
2 content to a client system if the client system has a limited-use client program and
3 wherein the limited-use client program limits reproduction of the content in at least one
4 way.

1 23. The method of claim 20, wherein the compensation is based on advertising
2 revenue obtained by the content provider based on advertising displayed in connection
3 with a user accessing content protected by the security system.

1 24. A method for controlling access to information presented by a web browser
2 comprising:
3 presenting content within a browser window of the web browser; and
4 disabling a disallowed user function when the content is within the browser
5 window.

1 25. The method of claim 24, wherein disabling the disallowed user function
2 comprises:
3 intercepting a message posted to the browser window; and
4 hiding the content if the browser is not a foreground application.

1 26. The method of claim 24, wherein disabling the disallowed user function
2 comprises:

3 clearing a commonly shared inter-application memory when the inter-application
4 memory is accessed.

1 27. The method of claim 24 wherein disabling the disallowed user function
2 comprises:

3 hiding a user menu selection corresponding to the disallowed user function.

1 28. The method of claim 24, wherein disabling the disallowed user function
2 comprises:

3 intercepting a keyboard message; and

4 discarding the keyboard message if it corresponds to the disallowed user function.

1 29. The method of claim 24, wherein disabling the disallowed user function
2 comprises:

3 monitoring a context for a device; and

4 discarding a user action directed to the device when the context matches the
5 content.

1 30. The method of claim 24, wherein the disallowed user function is one of a plurality
2 of default disallowed user functions and further comprising:

3 leaving active one of the plurality of default disallowed user functions.

1 31. The method of 30, further comprising providing information with the content that
2 determines the one of the plurality of default disallowed user functions to be left active.

1 32. The method of claim 24 wherein the disallowed user function is selected from the
2 group consisting of print, page setup, save, save as, view source, save picture as, set as
3 wallpaper, copy, screen capture, screen print, cut.

1 33. The method of claim 24 further comprising managing authentication of a web
2 client.

1 34. The method of claim 24 further comprising processing a request from a web client
2 for encrypted content.

1 35. The method of claim 24 further comprising creating a unique identifier for a web
2 client.

1 36. The method of claim 24 further comprising encrypting the content with a key
2 based on the unique identifier for the web client.

1 37. The method of claim 24 wherein the content comprises user perceivable
2 information in a hyper-text markup language (HTML) format.

1 38. The method of claim 24 wherein the content comprises user perceivable streaming
2 information.

1 39. The method of claim 24 wherein the content comprises at least one of video
2 information and audio information.

1 40. The method of claim 24 wherein the disallowed user function comprises a user
2 function which, when allowed, provides for non-ephemeral reproduction of the content.

1 42. The method of claim 24 wherein the content comprises user perceivable
2 information in a common gateway interface (CGI) language format.

1 43. The method of claim 24 wherein the content comprises user perceivable
2 information in a JAVA language format.

44. A computer-readable medium having stored thereon computer executable instructions to cause a client digital processing system and a server digital processing system to perform a method comprising:

- transmitting content from the server digital processing system to the client digital processing system over a network;
- presenting the content within a browser window on the client digital processing system; and
- disabling a disallowed user function when the content is within the browser window wherein the disallowed user function comprises a user function which, when allowed, provides for non-ephemeral reproduction of the content.

1 45. The computer-readable medium of claim 44 wherein disabling the disallowed user
2 function comprises:

3 intercepting a message posted to the browser window; and
4 hiding the content if the browser is not a foreground application.

1 46. The computer readable medium of claim 44 wherein disabling the disallowed user
2 function comprises:

3 clearing a commonly shared inter-application memory if the inter-application
4 memory is accessed.

1 47. The computer readable medium of claim 44 wherein disabling the disallowed user
2 function comprises:

3 hiding a user menu selection corresponding to the disallowed user function.

1 48. The computer readable medium of claim 44, wherein disabling the disallowed
2 user function comprises:

3 intercepting a keyboard message; and

4 discarding the keyboard message if it corresponds to the disallowed user function.

1 49. The computer readable medium of claim 44, wherein disabling the disallowed
2 user function comprises:

3 monitoring a context for a device; and

4 discarding a user action directed to the device when the context matches the
5 content.

1 50. The computer readable medium of claim 44 further comprising instructions to
2 cause the server digital processing system to manage the authentication of the client
3 digital processing system.

1 51. The computer readable medium of claim 44 further comprising instructions to
2 cause the server digital processing system to process a request from of the client digital
3 processing system for encrypted content.

660760-5042660
SUB
C2

a browser controller logically coupled to the message monitor to hide the content if the browser is not a foreground application.

57. The client digital processing system of claim 55, wherein the security module comprises a browser controller that clears a commonly shared inter-application memory when the inter-application memory is accessed.

58. The client digital processing system of claim 55, wherein the security module comprises a browser controller that encrypts the content.

59. A server digital processing system for controlling access to content distributed to a client digital processing system, the server digital processing system comprising:
a processor;
a network interface logically coupled to the processor to receive a request for the content from the client digital processing system;
a server module logically coupled to the network interface to distribute the content to the client digital processing system in response to the request; and
a security module logically coupled to the server module to determine if the request is from a client digital processing system executing a limited-use client program which prevents at least one form of non-ephemeral reproduction.

60. The server digital processing system of claim 59, wherein the security module is further operable to:
create a secure document object containing the content if the content is protected under an individual security model; and
pass the secure document object to the server module for distribution in response to the request.

1 61. The server digital processing system of claim 59, wherein the security module is
2 further operable to:
3 encrypt the content if the content is protected under a common security model;
4 and
5 pass the encrypted content to the server module for distribution in response to the
6 request.

sub C8 {
1 62. A computer-readable medium having stored thereon computer executable
2 instructions to cause a client digital processing system to perform a method comprising:
3 receiving protected content from a server digital processing system;
4 presenting the protected content within a browser window; and
5 disabling disallowed user functions when the protected content is in the browser
6 window wherein the disallowed user function comprises a user function which, when
7 allowed, provides for non-ephemeral reproduction of the content.

HP Contd
1 63. The computer-readable medium of claim 62 further comprising:
2 intercepting a message posted to the browser window; and
3 hiding the protected content if the browser is not a foreground application.

1 64. A computer readable medium of claim 62 wherein the disallowed user function is
2 enabled when content in the browser window is not designated to be protected such that
3 non-ephemeral reproduction of such content is allowed.

sub C9 {
1 65. A computer-readable medium having stored thereon computer executable
2 instructions to cause a server digital processing system to perform a method comprising:
3 receiving a request for protected content from a client digital processing system;

4 determining if the request is from a client digital processing system executing a
5 limited-use client program; and
6 distributing the protected content to the client digital processing system in
7 response to the request only if the client digital processing system is executing the
8 limited-use client program, wherein the limited-use client program prevents at least one
9 form of non-ephemeral reproduction of the protected content.

1 66. The computer-readable medium of claim 65, further comprising:
2 creating a secure document object containing the protected content if the content
3 is protected under an individual security model; and
4 passing the secure document object to the server module for distribution in
5 response to the request.

1 67. The computer-readable medium of claim 65 further comprising:
2 encrypting the protected content if the content is protected under a common
3 security model; and
4 passing the encrypted content to the server module for distribution in response to
5 the request.

1 68. A computer readable medium of claim 65 wherein the limited-use client program
2 disables a disallowed user function that comprises a user function which, when allowed,
3 provides for non-ephemeral reproduction of the content.

1 69. A computer readable medium of claim 68 wherein the disallowed user function is
2 enabled when content is not designated to be protected such that non-ephemeral
3 reproduction of such content is allowed.

1 70. A computer readable medium of claim 69 wherein non-ephemeral reproduction of
2 the protected content is allowed after a transaction between the client digital processing
3 system and the server digital processing system.

1 71. A computer readable medium of claim 70 wherein the transaction comprises at
2 least one of a compensation to a provider of the protected content or an exchange of
3 identification of the client digital processing system.

1 72. A computer readable medium having stored thereon a secure document package
2 data structure comprising:
3 a document package header field containing data representing a description for the
4 secure document package;
5 a delivery object field containing data representing executable code to manage the
6 secure document package described by the document package header field; and
7 a document field containing data representing content contained in the secure
8 document package described by the document package header field.

1 73. The computer readable medium of claim 72, wherein the document package
2 header field comprises:
3 a package identifier field containing data representing an identifier for the secure
4 document package.

1 74. The computer readable medium of claim 72, wherein the document field
2 comprises:
3 a document identifier field containing data representing an identifier for the
4 content.

660760" 5012660

1 75. A computer data signal embodied in a carrier wave and encoding a data structure
2 containing protected content comprising:
3 a document package header field containing data representing a description for the
4 secure document package;
5 a delivery object field containing data representing executable code to manage the
6 secure document package described by the document package header field; and
7 a document field containing data representing content contained in the secure
8 document package described by the document package header field.

1 76. The computer readable medium of claim 75, wherein the document package
2 header field comprises:
3 a package identifier field containing data representing an identifier for the secure
4 document package.

1 77. The computer readable medium of claim 75, wherein the document field
2 comprises:
3 a document identifier field containing data representing an identifier for the
4 content.

sub
c10
1 78. A system for controlling reproduction of content on a client computer comprising:
2 means for receiving content to be protected; and
3 means for displaying the protected content on the client computer while
4 preventing at least one form of reproduction of the content.

H
Contd
1 79. The system of claim 78, wherein the means for displaying comprises:
2 means for disabling user functions that reproduce the content.

H1
Cont'd

1 80. The system of claim 79, wherein the means for displaying further comprises:
2 means for enabling disabled user functions under pre-determined conditions.

sub
CH

1 81. A system for controlling reproduction of content stored on a server computer
2 comprising:
3 means for protecting content stored on the server;
4 means for receiving a request for the protected content; and
5 means for determining if the request is from a requestor that limits reproduction of
6 protected content.

1 82. The system of claim 81, wherein the means for protecting comprises:
2 means for creating a secure document object containing the content.

1 83. The system of claim 81, wherein the means for protecting comprises:
2 means for encrypting the content.

ADD
C2
ADD E